Kai Wittig

Chapter 6. Privacy in Social Networks After the Global Surveillance Disclosures

Abstract: In May 2013, Edward Snowden disclosed U.S. federal government information to the media, highlighting global surveillance activities concerning operations conducted by the National Security Agency, in addition to other secret service operations regarding the monitoring of most parts of the Web, especially social networks. Privacy concerns on the Internet have thus been highly affected because of his actions. Investigating the consequences of this behavior as regards users of social networks is of primary interest. Do users care about their online privacy? Are they honest about the data they post? Do they believe their online data are safe? If not, what actions do they take to minimize the risks of privacy violations? Does a "pushback" phenomenon exist?

To answer these questions, we conducted an empirical study between 22 July and 11 August 2014. The method used was an online questionnaire (in German) that was spread across German web-forums and social media networks. There were 304 people who participated in this study. Participants were grouped by sex, age, and educational background, and asked about their behavior in online social media networks and their subjective feelings toward online privacy.

Most results of previous studies concerning self-revelation on social networks could be verified: for example, the differentiation between more and less intimate personal information. On the one hand, results demonstrate most users willingly share their real personal information. Furthermore, a strong correlation was found between the level of self-revelation on social media and age, as well as sex. On the other hands, educational background does not seem to affect the participant's behavior concerning self-revelation. An awareness of the problem toward privacy violations does slightly correlate with age and education. The most common method to protect one's online privacy is to limit the range of information spread to special groups (e.g., close friends). Only very few participants stated they are using encryption in their online communications.

"Pushback" behavior in direct context with these global surveillance disclosures could not be documented. Users know about the risks but seem willing to ignore them when weighed against the benefits gained from using social media. This study therefore concludes that a need does exist to act on the growing aware-

Kai Wittig, Department of Information Science, Heinrich-Heine-University Düsseldorf, Germany, Kai.Wittig@hhu.de

ness concerning privacy matters on the Internet, especially as it pertains to young people.

Keywords: privacy; social media; surveillance disclosures; NSA; push-back.

Introduction

On June 9, 2013, U.S. federal government contractor Edward Snowden posted a video interview on the Internet site YouTube in which he outlined his motives for disclosing internal federal government documents of the U.S. National Security Agency (NSA) to the public. These documents were subsequently analyzed and published in both the British *Guardian* and the *Washington Post* newspapers. Over the next several months, until 2014, new facts concerning the extent of NSA's monitoring capabilities regarding public conversations, over the Internet and the telephone lines, continued to emerge.

By exposing the agency's use of PRISM, a tool whose existence was confirmed by NSA itself (Thoma & Greis, 2013), came the knowledge that the agency is and had been systematically monitoring large segments of the Internet. The largest Internet companies in the United States, including social networking services (SNSs), such as Facebook and Google Plus, were also involved in the project (O'Harrow Jr. et al., 2013). Thus, it also came to be known not only how NSA collects social network metadata, but also the communication content within these data (Eiermann, 2013).

A representative study conducted between May and April 2014 in Germany (DIVSI, 2014) concluded a majority of Germans (56 %) indeed believe that everyone is being wiretapped, but only 9 % of respondents note they are being "much more careful" on the Internet. This chapter aims to empirically examine whether changes have occurred regarding the handling of privacy in social media resulting from Edward Snowden publishing information about NSA actions undertaken to monitor private individuals' data, as well as similar actions conducted by other intelligence agencies.

Privacy

The Definition of Privacy

We ask, first, what is privacy? Alan F. Westin defines privacy as follows: "The claim of an individual to determine what information about himself or herself should be known to others" (Westin, 1967; 2003, p. 7). This definition contains two important aspects. First, an individual's privacy must be divided into and distinguished from the concept of private and non-private information. Second, each person decides on an individual basis how to make such a distinction. Rössler (2001) states: "The dividing line between what is designed as public, and what is to be considered private is not fixed; the boundaries are up for debate, even in liberal societies."

Privacy therefore does not mean to keep all information to oneself or to foreclose on society's ability to learn about an individual's life. Rather, it concerns controlling the use of one's own data and determining to whom one might reveal such information, and under which terms others may own or make use of another person's specific personal information (Schenk et al., 2012).

Privacy can be separated into four dimensions (Burgoon et al., 1989): *physical*, *interactional*, *psychological*, and *informational*. Physical privacy means the "freedom from surveillance and unwanted intrusions upon one's space by the physical presence" (Burgoon et al., 1989, p. 3). Interactional (also social) privacy describes the control an individual or a group takes concerning with whom, about what, and when social exchange processes occur. Psychological privacy means the right to control which and whether data will be made public. Type and volume of information matter in this context. It is also important to protect one's own thoughts from outside influence: "Psychological privacy is particularly relevant and endangered on the social web" (Schenk et al., 2012, p. 40). Informational privacy is described by Burgoon et al. (1989) as the control about whom and under which circumstances someone's private information is collected, used, or distributed. Rössler writes: "A piece of information is considered private if you can regulate the access to it" (2001, p. 23).

Both Burgoon et al. (1989) and Cho and Larose (1999) note interventions in all areas of privacy are perceived by individuals during which "infringements on informational and psychological privacy are the most offensive" (Cho & Larose, 1999, p. 422). Westin (1967) further describes the concept of people's privacy having four major functions: 1) it allows personal autonomy, 2) it provides emotional relief, 3) it offers an important part of self-evaluation, and 4) it enables sharing of intimate information within a private circle.

A person can feel she has too little or too much privacy. Someone whose private life is discussed in public may feel he has too little privacy, whereas someone whose possibilities to inform other people are constrained may feel she has too much. "The regulation of privacy is neither static nor rule governed but instead takes place depending on the immediate social context" (Schenk et al., 2012, p. 41). In one study, it was shown that individuals regulate the amount of privacy they perceived as pleasant, ranging from "Openness" to "Closedness" by constantly adapting this range due to internal and external influences (Altman, 1977). Openness or even self-revelation by one party in a conversation can lead others to behave more willingly and open themselves in return (Cozby, 1973).

According to Petronios' "Privacy Management Theory" (2002), every person has a "Rule-Based Management System" regulating the degree of openness or closedness. Individual rules are created, depending on context, and these are influenced by culture, gender, motivation, and a cost-benefit analysis. Once a piece of information is shared, however, there is at least one co-owner. From the perspective of the original owner, certain liabilities also apply to the co-owner. These liabilities are negotiated as rules between the two participants. Especially in social networks, complying with these rules – by both other users and the operating company – is particularly important because users rely on such mutual compliance for protecting their private data.

Privacy Characteristics in Social Networks

Having clarified the notion of privacy in general, we turn to the specific characteristics of privacy within social networks. Studies of Joinson in 2001 and Taddicken in 2008 indicated an increased openness and willingness to provide information in online communication compared with direct, face-to-face communication: "Due to anonymity and the lack of gestures, facial expressions, and voice in primarily text-based online communication, users compensate for the information-poor environment through increased disclosure" (Schenk et al., 2012, p. 43). Furthermore, there are five differences in "network publics" (Boyd & Marwick, 2011) compared with face-to-face communication:

- Persistence: online expressions are automatically recorded and archived.
- Replicability: content made out of bits can be duplicated.
- Scalability: the potential visibility of content in networked publics is great.
- Searchability: content in networked publics can be accessed through searches.
- Invisible audiences: not all audiences are visible when a person is contributing online, nor are they necessarily co-present (Boyd, 2008).

Because of these differences regarding offline communication, in particular, for Points 2 and 3, self-revelation on the social web can be taken out of the context in which such a decision was originally made. This effect is called "recontextualization" (Taddicken, 2010).

"Publicity by default" is another characteristic of social media. Most SNSs, such as Facebook, by default make all user-created profiles and accompanying information available to "the public," means anyone can view another's data. Users who upload data to the SNS must take action to change the public availability of their personal data by using privacy settings. Via these settings, an individual's privacy can be secured to a certain extent. The user, however, must maintain a continuous vigilance over their information and choose between qualities of being open or closed to participate in the social media sphere: "Maintaining a degree of privacy, or 'closedness,' will often require disclosure of [one's] personal information or whereabouts" (Palen & Dourish, 2003, p. 3).

It remains that even if a piece of information is revealed only to a limited circle, for example, to one's closest friends, an invasion of privacy may still occur. This occurs when co-owners of the information fail to follow the agreed-upon rules and spread the information, knowingly or unknowingly. This can cause problems in some situations (Margulis, 2003, p. 247 f.).

According to research from the United States, different users perceive such threats in different ways, with researchers separating them into three categories: "privacy fundamentalists" who feel privacy is very important; the "unconcerned," who feel little or no worry about their online privacy; and "privacy pragmatists," who feel online privacy is important and therefore attempt to protect it. Surveys reveal the third group makes up a 64 % share (Wildemuth, 2006).

Dealing with Privacy in Social Networks

In recent years, many empirical studies have discussed how users deal with their privacy in social networks. Being active in any social network means being willing to share some amount self-revelation as a necessary condition to belong (Taddicken & Jers, 2011). Most studies of self-revelation in social media focus on the information provided by users of these networks in their respective profiles. Research has revealed most users offer more information about themselves than usually occurs in face-to-face conversations (Christofides et al., 2009; Haferkamp, 2010). Information provided in the profiles can be ordered by intimacy: data often revealed, such as a person's first name or gender, are considered less intimate than, for example, a personal telephone number or an exact address (Boyle & Johnson, 2010). Among the data most often released are the last name

and a photo of the user (Prommer et al., 2009). Most users do not provide direct contact information (Taraszow et al., 2010) because it results in an increased risk of abuse by publishing more intimate data (Taddicken, 2010).

There is a correlation between quantity of the revealed data and level of intimacy. A user who shares a greater amount of information also usually shares a more intimate type (Nosko et al., 2010). Studies on gender with regard to the veracity of social media profiles concluded men use social networks more openly than women do (Prommer et al., 2009), and men are also more likely to share their contact information (Taraszow et al., 2010).

Overall, it can be stated that "the personal profile in a social network is an important aspect of online self-revelation" (Schenk et al., 2012 p. 49). Nevertheless, it should be noted that creating and maintaining custom profiles is a reflective action, which usually takes place on first entering a network when the user is made aware of deciding which data he wants to publish or which to keep (partially) private.

Profiles are not the only spaces where private information can be revealed on social networks. Additional features, such as tagging of people in uploaded photos, organizing posts or photos into groups, writing on other peoples' profiles, and linking of organizations or individuals are also part of one's online identity and these spaces can also lead to increased opportunities for further self-revelation. Such so-called "dynamic contents" becomes even more important as it forms part of how others perceive a given individual on the social web (Boyd & Marwick, 2011). Information such as accepted friend requests and "likes" are less active parts of self-revelation and potentially less obvious to the user.

In addition to the amount and degree of intimacy of published information, accessibility plays an important role: "Self-representation does not take place without context, but always in response to an audience" (Schenk et al., 2012, p. 50). The user establishes her audience by the particular privacy settings she turns on or off within the network. A 2011 study from the United Kingdom demonstrated users rarely review their privacy settings, even if the SNS changes them. Furthermore, a user's desired settings often do not match those he actually sets (Butler et al., 2011). Another study shows students keep their profiles mostly private, if they are female, very active, and have friends who have adjusted their privacy settings to be restrictive (Lewis et al., 2008). In general, user experience on the social web seems to be strongly influenced by the active use of privacy settings. In 2006 and 2007, Patchin and Hinduja conducted a longitudinal study of privacy behavior on MySpace.com and concluded that within one year, the share of those who kept private their profiles had risen significantly (Patchin & Hinduja, 2010).

Most of these studies draw their data from the United States and the United Kingdom, and, due to cultural differences, their findings cannot be transferred to users in Germany. One study of BITKOM (a federal association for Information Technology, Telecommunication and New Media), from 2011 shows the German people take their privacy in social networks extremely seriously: 86 % of survey respondents have dealt with privacy settings in the past, with 77 % changing them. Only 11 % did not treat the issue of privacy settings (BITKOM, 2011). The same survey also showed young people (under 30) find their privacy very important. Indeed, an awareness for online privacy within the past few years seems to have increased rather than decreased (Utz & Kramer, 2009). This trend can be observed in the United States as well (Boyd & Hargittai, 2010).

The Privacy Paradox

The *privacy paradox* is a term coined by Susan B. Barnes (2006) to describe a phenomenon she has observed in surveys. While most users (in Barnes' study, adolescents) set a high value on protecting privacy on social media sites, they do not always behave accordingly, putting their personal information voluntarily in front of the public eye (cf. Butler et al., 2011). One can assume that almost all users are by now aware of the dangers of online self-revelation, yet do not want to give up the advantages of social media, whether from peer pressure or for other reasons.

One possible explanation for the privacy paradox is users may split their privacy into two parts when it concerns online privacy (Schenk et al., 2012): privacy within their social environment and privacy toward foreign persons and companies or institutions. The former relates to social privacy; the latter, to the informational. The user might underrate the risk of interventions in informal privacy by the provider of the social network.

Threat to Privacy by Providers and Secret Services

In centrally managed social networks, informational privacy is already jeopardized by the very existence of a provider, on whom users must rely. Facebook and other social networks have extensive rights to the use of all uploaded data, stipulated according to their terms of service. The use of these services is usually free, and the provider earns money by including advertising on users' site pages. Especially in the United States, networks operate under extremely lax privacy policies compared with those of Europe (Stiftung Warentest, 2010). In addition,

it is in providers' best interests that users are encouraged to enter the maximum amount of data or information about themselves and their activities, interests, and so forth. The more data is available to the network, the better and more precisely targeted advertisements can be, which in turn increases the company's or network's advertising revenue.

With regard to wiretapping by government agencies or secret services, as introduced at the beginning of this chapter, it must be assumed that, at a minimum, users' informational privacy is being actively violated. This intervention of people's privacy should not be taken lightly: "The autonomy of a person may be injured, damaged in ways that do not affect the rights of freedom itself immediately: and because of these opportunities, people, in their autonomy, must rely on the protection of the private sphere" (Rössler, 2001, p. 26).

Empirical Investigation

Research Questions

Having described the importance of privacy in general, and particularly within social networks, and also the treatment thereof due to the potential for surveillance by government intelligence services, as well as presenting the state of scientific knowledge and current studies about it, we present our research questions (RQs) on which we base our empirical study. The overarching question is "Have the global surveillance disclosures by Edward Snowden led to changes in using social media?" This leads to the first RQ:

RQ1: To what extent do users reveal themselves on social networks and if so, do they enter their data truthfully?
The risks of self-revelation on the network have been established sufficiently in the previous sections of this chapter. By using the services and accepting the related agreement of terms and conditions, the user submits his informal self-determination to the provider and its advertising partners, and by extension, government intelligence services.

To investigate the extent to which the privacy of users is at risk, we must first ascertain whether such risk exists at all. On the one hand, social media users who falsify their data partially or completely, in which they have neither name nor address or other personally identifiable information, such as photos and videos, will experience little to no risk of privacy violations. On the other hand, choosing to upload little data makes it difficult for them to enjoy a meaningful online social

life (Taddicken & Jers, 2011). In this context, we found it interesting to examine which kinds of information are treated more openly by users or which remain strictly private. This leads to the following two RQs:

RQ2: Do users care about privacy settings in social networks?
RQ3: Do users check these settings prior to uploading data?
These two RQs are directly related to studies made by Lewis et al. (2008) and Butler et al. (2011). It is especially interesting to learn if the results from these studies can be transferred to German users or if the results of the 2011 BITKOM study, which revealed an increasing skepticism about online self-revelation, correspond more to this empirical investigation. We come to our fourth RQ:

RQ4: How safe do users feel their data are on the Internet?
This RQ examines whether there is an awareness among participants concerning any danger posed by published information on the Internet, and refers to studies such as that by Wagner, Brüggen, and Gebel (2010) and many others. Stemming in part from the security breach of Snowden and his subsequent publishing of NSA data, one can presume that users have a more limited trust in Internet privacy. This leads to our fifth RQ:

RQ5: Which methods do users apply to secure their online privacy?
Users have some methods at their disposal to protect their privacy while on social networks. Studies have shown many users are aware of the dangers of self-publication (e.g., Christofides et al., 2009) and act at least, in part, accordingly. This RQ is aimed at the mechanisms that are used to achieve it. Five common methods were listed on the questionnaire to choose from; in addition, a free text field was available to add further methods or information. We next offer our sixth RQ:

RQ6: Do users apply encrypting tools to make it difficult for others to monitor them?
Software for SNSs, such as Facebook, is available that uses encryption algorithms to secure information from wiretapping. However, these tools are exclusively linked to private communications within the networks (e.g., private messages, chats) and offer no protection for public information that applies across the network, even if the data are available only to a small circle of friends via privacy settings. For private communication within networks, which is monitored automatically (Pauker, 2012), these programs offer protection against wiretapping by both the provider as well as intelligence services. We present our seventh RQ:

RQ7: Is there a pushback movement due to Snowden's leaks?
Are privacy violations a cause for pushback behavior (Morrison & Gomez, 2014)? It is interesting to learn whether any participants in our study canceled their membership on social networks because of publications about surveillance conducted by government intelligence services. If so, which memberships are subject to this effect? This leads to our ninth RQ:

RQ8: Are there any differences concerning privacy protection on social media sites with regard to age, gender, or educational background?
A 2010 study by Wagner, Brüggen, and Gebel showed that age plays a role when dealing with the risks of social networks. The results reveal younger users are less concerned with sensitive information than older users are. Gender plays an interesting role as well: men are often more open to share information than women are (Lewis et al., 2008; Prommer et al., 2009). It will be interesting to examine, over the long term, if and to what extent Snowden's disclosures affect self-revelation. As a further feature, educational level can be used. It is expected that better-educated users act more prudently when it comes to privacy. All three demographic dimensions were polled during this study and thus flow into our evaluation.

Methods

To answer these research questions, a quantitative data acquisition method was used. An online questionnaire was created with the help of online tools from umfrageonline.com. This questionnaire was then distributed over a link in various ways on the Internet to obtain the largest possible number and range of participants. A disadvantage must be cited: As with all online surveys, only participants who are also Internet users could enroll in the survey. This disadvantage is not significant for this study because participants who use social media must by definition be Internet users.

Because of its scope and number of responses, this study cannot be considered as representative for all of Germany. However, it can indicate more than certain tendencies and confirm or refute results of previous studies. The survey ran from 22 July to 11 August 2014, and completed a feedback index of 326 responses, although only 304 participants answered all the questions. Incomplete questionnaires were excluded from the analysis, so the study was carried out with a group size of $n = 304$.

Participants

As noted, the survey was distributed throughout various Internet channels to obtain a widest possible participant field. The link to the survey could be found on various Internet forums, chat rooms, and social media sites, like Facebook and Twitter. There was no payment offered for participating. Of the 304 participants, 75 % (229) were male, 23 % (69) female, and 2 % (6) did not specify gender (see Figure 1). The average age was 28.49 years (within a range of 14–71 years). In order to incorporate age as a criterion in evaluating the records, participants were divided into three age groups, with the breakdown distinguishing between "digital natives" and "digital immigrants." Participants are considered digital natives if they are between 14 and 29 years old, were born after 1985, and therefore grew up during or after the spread of the Internet (n = 203). Participants older than 35 years or older are digital immigrants, were born before 1980, and spent a youth absent of the Internet or other kinds of online information technology services (n = 53). The third group is a buffer or buffer group. It includes all participants between the ages of 30 and 35. These users have experienced the rise of information technology, but are not necessarily strongly influenced by it.

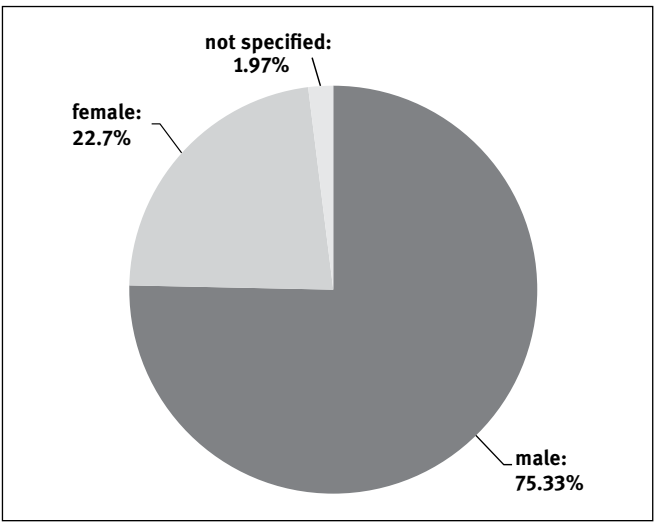

Figure 1: Distribution by Gender.

The education level shows the following distribution (see Table 1). It should be noted that students who are currently attending school may have selected "no degree" category.

Table 1: Distribution by Educational Level.

Distribution by education level		
	Number (n=304)	Percentage
Without graduation	19	6,3
Certificate of Secondary	12	3,9
Junior high school	38	12,5
University-entrance diploma ('Abitur')	123	40,5
Academical grade	86	28,3
No answer	26	8,6
Total	304	100,0

Results

Distribution of Social Networks Among Participants

The first question of the survey asks about the participant's membership on the different social media sites. The results reinforce the dominant position of Facebook.

Table 2: Distribution of Social Media Sites.

Distribution of social media portals		
	Number (n=304)	Percentage
Facebook	230	75,66
Google+	69	22,70
Twitter	108	35,53
Xing	50	16,45
linkedIn	8	2,63
Flickr	25	8,22
Youtube	184	60,53
Tumblr	10	3,29

Tab. 2 (continued)

Distribution of social media portals		
instagram	4	1,32
VK	3	0,99

Degree of Self-Revelation by Sex, Age Group, and Educational Level

The next question is concerned with the degree of self-revelation within social networks. The participants were asked how they revealed four characteristics (name, photo, date of birth, place of residence), which are present in all social networks. They were informed to solely count truthful declarations. These four pieces of information can be divided into two categories: name and photo are considered not very intimate, while the date of birth and place of residence as part of the address can be regarded as intimate information (see Boyle & Johnson, 2010).

These data confirm the results of Boyle and Johnson in 2010 (see Figure 2). Both the name and a picture are significantly more often revealed truthfully than are the date of birth and place of residence.

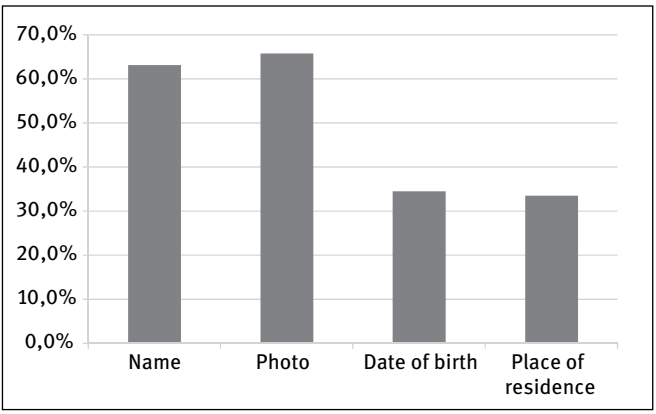

Figure 2: Self-Revelation on Social Media.

By analyzing the self-publication by gender, we observe female users divulge more information in each category than men do (see Figure 3). This contradicts

previous studies that women are less willing to self-publish in social networks than men are (see Lewis et al., 2008; Prommer et al., 2009).

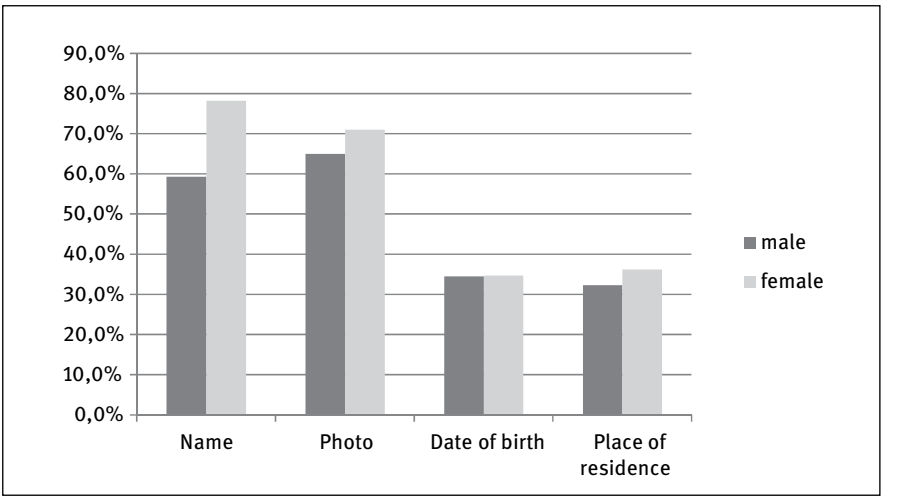

Figure 3: Self-Revelation by Gender.

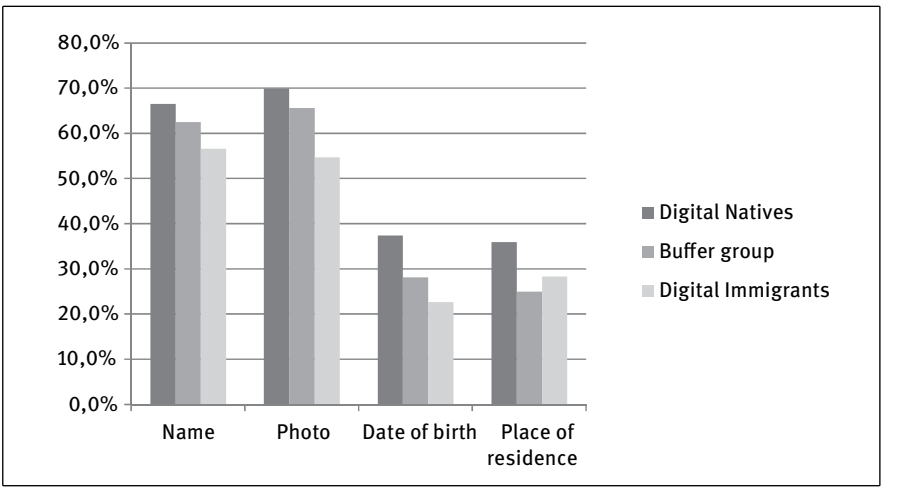

Figure 4: Self-Revelation by age groups.

In each category, women supply their personal information more truthfully than men do. It should be noted, however, that comparing the results can only

be done relatively because of gender inequality in the number of participants. Broken down by age group, the data display a gradient of young to old (see Figure 4). Thus, it is likely awareness concerning the dangers of online self-expression increases with age. This gradient also confirms the results from a 2012 study by Schenk et al. (cf. Schenk et al., 2012, p. 144).

To investigate further research hypotheses, the questions regarding self-revelation were summarized in an index. The binary data from the questionnaire (1 = "information divulged," 0 = "information not divulged") were summed to a single value (hereafter, self-revelation or SR index). The span of the self-revelation of the SR index is therefore between 0 and 4, where 0 means the participant did not divulge any information, while 4 means he or she shared all information.

Examining the SR index with respect to participant age, the results indicate a strong negative correlation (see Table 3).

Table 3: Correlation of SR Index and age. **. Correlation is significant at the 0.01 level (two-tailed).

		SR-Index	**Age**
SR-Index	Pearson Correlation	1	–,159**
	Significance (2-tailed)		,007
	N	304	288
Age	Pearson Correlation	–,159**	1
	Significance (2-tailed)	,007	
	N	288	288

The degree of self-revelation stands in an inverse relationship to age.
The negative correlation is significant in this case and shows that a willingness to self-reveal declines with age. The correlation can be found by exact age as well as by age group.

Education level also was summed to an index. The range is from 1 to 5, where 1 means no degree, while 5 stands for an academic certificate. Participants who did not state their educational level are not included in the educational index, since there may be several reasons they did not disclose this part of information.

The degree of self-revelation is not related to the education level.
However, the underlying data but does not indicate a correlation between the level of education and self-revelation (see Table 4). This is surprising, because previous studies have shown highly significant correlations in this area (cf. Taddicken, 2011, p. 293).

Table 4: Correlation of SR Index and Education Index.

		SR-Index	Education-Index
SR-Index	Pearson Correlation	1	,004
	Significance (2-tailed)		,946
	N	304	278
Education-Index	Pearson Correlation	,004	1
	Significance (2-tailed)	,946	
	N	278	278

Privacy Settings and Their Use

When asked how intensively they deal with the privacy settings of social media services, most participants stated they deal at least occasionally with the matter (73 %). Of participants, 27 % state they are often concerned with the privacy settings, and 18.4 %, allegedly, all the time. On the opposite side, 23.4 % are rarely and 3.6 % are not at all concerned with these settings (see Figure 5).

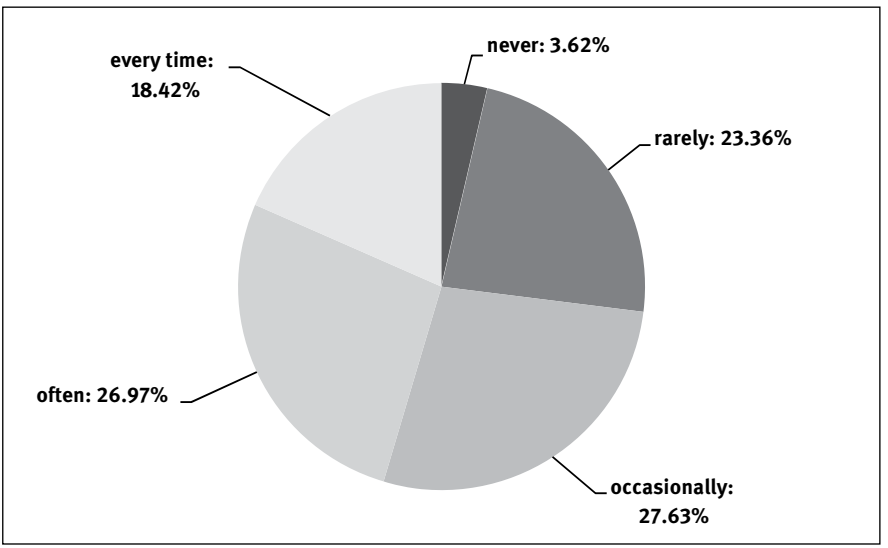

Figure 5: Privacy Settings' Usage.

The answer to the question about reviewing visibility settings before posting offers a similar result: the vast majority of participants check the settings before each post (77 %); with 16.8 % reporting not doing so, and 6.3 % indicating they do not know how to do so. For these data, we created a corresponding index (Privacy Settings or PS index). It is designed to investigate correlations with age, sex, and education. Our results demonstrate the PS index correlates positively with both age and level of education (see Tables 5 and 6).

The use of the privacy settings is positively related to age.

The use of the privacy settings is positively related to educational level.

Table 5: Correlation of PS Index and age. **. Correlation is significant at the 0.01 level (two-tailed).

		PS-Index	**Age**
PS-Index	Pearson Correlation	1	,194**
	Significance (2-tailed)		,001
	N	304	288
Age	Pearson Correlation	,194**	1
	Significance (2-tailed)	,001	
	N	288	288

Table 6: Correlation of PS Index and Education Index. **. Correlation is significant at the 0.01 level (two-tailed).

		PS-Index	**Education-Index**
PS-Index	Pearson Correlation	1	,259**
	Significance (2-tailed)		,000
	N	304	278
Education-Index	Pearson Correlation	,259**	1
	Significance (2-tailed)	,000	
	N	278	278

There are no correlations between the PS index and gender (see Figure 6). Only the two extremes reveal tendencies toward female participants being more concerned about their privacy. Here again, we note these data should be considered in light of the unequal participant distribution and therefore can hardly generate relevant statements.

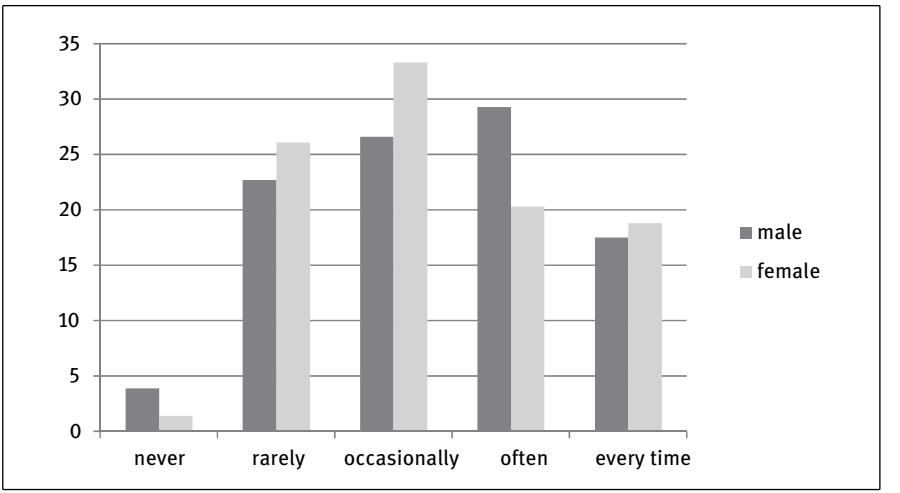

Figure 6: Privacy Settings' Usage by Gender.

The question of whether the participant has changed his privacy settings within the last 12 months (which corresponds approximately to the period between Snowden's releases and the start of our survey) found 65 % of respondents answering "yes" and 35 % "no." This coincides roughly with the previous figures: "rarely" and "never" were stated, in the aggregate, by approximately 27 % of respondents. The difference of 35 % can be explained by varying interpretations of the word "occasionally."

Encrypting Communication

One way to protect against surveillance and thus an invasion of privacy is to encrypt data. This refers, as mentioned above, only to direct communication between two individuals within a social network and not to information that is available within the profiles and as a consequence across the SNS. Of respondents, 87.5 % stated they never used encryption within social media services, 6.9 % have tested encryption tools at least once, 2 % use them occasionally, and 3.6 % report regular use. When asked about their encryption tool, most of those who did use one declared they used the Off-the-Record (OTR) protocol. Due to the low response rate for this question, it is not worthwhile checking for correlations with other factors.

Subjective Perception of Data Security by Respondents

In the following question, participants were asked to decide how safe they perceive their data are on the Internet and provide their answers using a scale ranging from 0 to 100. The question was deliberately left open-ended, and at this point in the questionnaire, Edward Snowden and intelligence services had not yet been mentioned. We wanted users to be influenced in their answers as little as possible.

The distribution of all participants can be seen in Figure 7. Regarding gender, there are hardly any differences. It must be stated, however, that most respondents perceive their data as very uncertain on the Internet (arithmetic mean: 26.22 on a scale from 0 to 100 from "unsafe" to "safe"). The mean absolute deviation is 17.64; the standard deviation, 22.81.

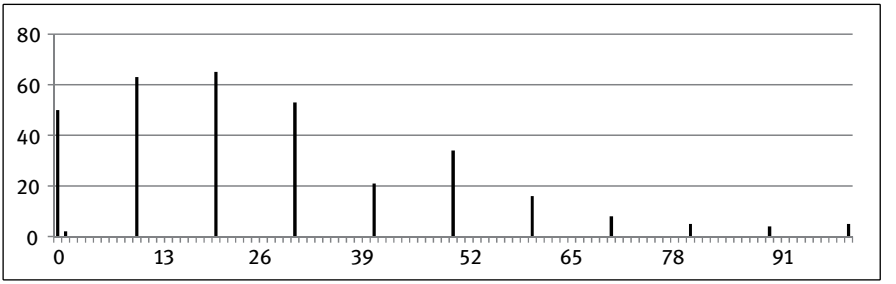

Figure 7: Distribution of experienced Data Safety on the Internet.

With respect to previous data, we found interesting results: They do not correlate significantly with the SR index, although they do correlate slightly negatively with age and the educational index.

It can be stated an awareness concerning privacy exists among participants. This also increases with age (see Table 7) and with educational level (see Table 8). In connection with self-revelation, no significant correlation could be found. One can presume a certain amount of self-revelation is regarded as somewhat necessary for membership in social networks. Our results confirm the widely established privacy paradox (see section above, this chapter).

The perception of low data security in the Internet is in a slightly negative correlation to age.

The perception of low data security in the Internet is in a slightly negative correlation to education.

The perception of low data security in the Internet is not related to online self-revelation.

Table 7: Correlation of Data Security Index and age. **. Correlation is significant at the 0.01 level (two-tailed).

		DS-Index	Age
DS-Index	Pearson Correlation	1	–,117**
	Significance (2-tailed)		,047
	N	304	288
Age	Pearson Correlation	–,117**	1
	Significance (2-tailed)	,047	
	N	288	288

Table 8: Correlation of Data Security Index and Education Index. *. Correlation is significant at the 0.05 level (two-tailed).

		DS-Index	Education-Index
DS-Index	Pearson Correlation	1	–,154*
	Significance (2-tailed)		,010
	N	304	278
Education-Index	Pearson Correlation	–,154*	1
	Significance (2-tailed)	,010	
	N	278	278

Methods to Secure Privacy

Having established there is a strong awareness of the dangers of self-revelation among participants, one should examine whether the risk of monitoring directly affects respondents' behavior. In total, just over a quarter of respondents (27.3 %) stated they had changed their behavior at least somewhat due to Snowden's revelations regarding online social media. The remaining users felt either little (54.3 %) or no (18.4 %) reason to take any action (see Figure 8).

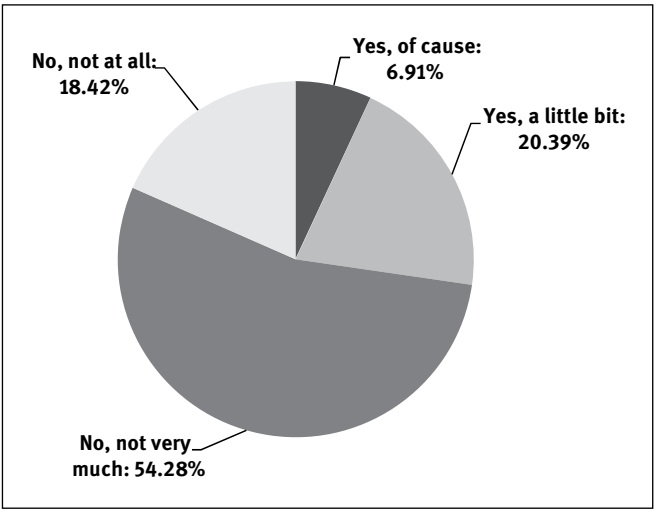

Figure 8: Changed Behavior in Social Media due to Snowden Disclosures.

The numbers for changed behavior (CB index) correlate significantly with neither age nor education (see Table 9). In this case, this can be justified by the small number of positive responses.

Table 9: Correlation of CB Index to Education Index and age. **. Correlation is significant at the 0.01 level (two-tailed).

		CB-Index	Education-Index	Age
CB-Index	Pearson Correlation	1	–,048	,064
	Significance (2-tailed)		,428	,280
	N	304	278	288
Education-Index	Pearson Correlation	–,048	1	,322**
	Significance (2-tailed)	,428		,000
	N	278	278	268
Age	Pearson Correlation	,064	,322**	1
	Significance (2-tailed)	,280	,000	
	N	288	268	288

Change of behavior regarding social media is not related to age.
Change of behavior regarding social media is not related to education.

Participants who responded "yes" to the question on changing behavior were asked in the subsequent question how doing so manifests itself (multiple answers were possible). Of participants, 56.1 % reported they upload less data, and 40.2 % have limited the visibility of their personal information to friends only. The latter is a popular but deceptive method. It aids only against privacy attacks from other users and even then, only if one has chosen one's friends wisely. Against the network provider and intelligence services, it has no effect. Furthermore, there is always the risk of privacy violation by co-owners: 34.1 % have had their data deleted, wholly or partially; 26.8 % have falsified their data; and 39 % stated they contact friends via different communication channels.

No Increased Pushback Behavior

When asked whether the participant had canceled any social media memberships in direct connection with the surveillance disclosures, only 19 people (6.3 %) answered in the affirmative. Of these 19, 10 declared they had closed their Facebook account, and 2 closed all but the Facebook account.

Even within this relatively small study, this group can be considered marginal. In addition, it also repeatedly comes down to fluctuations in the number of members on Facebook, regardless of surveillance disclosures. There has been some discussion in media in general and on Facebook in particular about a general decline in the site's membership, particularly among very young users (Spiegel Online, 2013). These results in connection with the data described in section above, this chapter, illustrate once more the privacy paradox effect.

Challenges and Prospects

The most difficult part of conducting the study was distributing the questionnaire. It was not easy to find participants. In social networks, such requests tend to go unseen due to the constant flood of information. In forums, such "beggar-posts" are unwelcome. Many of the posts soliciting participants for this survey were quickly deleted by moderators. The target of securing at least 500 respondents was missed. Some participants thus came from the immediate environment, as well as from their friends and acquaintances.

The reason for gender inequality is that most thematically appropriate forums were those that are very technology oriented. Experience has shown these forums are frequented more often by men than by women. To compensate for this occurrence, we also took care to visit forums with a high proportion of women (e.g., kleiderkreisel.de). Unfortunately, the response rates were lower in these environments. As a consequence of this unequal distribution, a satisfactory examination of the individual criteria by gender was possible; however, due to the small amount, it was often hardly meaningful and therefore useless ($n < 50$).

As part of the evaluation, it was observed that some questions in the questionnaire ought to have been more detailed, for example, Questions 2 and 4. Instead of querying the answers as Boolean values, scales (maybe 1–5) would have allowed for an even deeper analysis. The danger is that more questions deter ever more potential participants, which in turn leads to even less representative results.

It would have been interesting to procure a longitudinal study with a similar or the same survey immediately after the first publications of Snowden's disclosures. Such results compared with those found in this study could have indicated a trend. A future study, however, may be equally interesting and enlightening.

Conclusion

In the recent past, the self-revelation behavior of social media users has been extensively investigated by scientists. New in our present study is the investigation of a direct link between the acute danger of data espionage by intelligence services and users' subsequent reaction to that danger. Using the available data, our core question asking have users changed their behavior in response to the Snowden disclosures about social media surveillance can be denied with a high probability. However, these data can retrace the results of other studies: The distribution of personal information via intimate and less intimate information has been confirmed (cf. Schenk et al., 2012).

Furthermore, significant correlations between the degree of self-revelation and the age of the users were noted, but not between levels of self-revelation and education (cf. Taddicken, 2011). In addition, correlations were found between the subjective perception of data safety, and age and educational level. The share of users who enter their data truthfully is surprisingly high. It is presumed that social media providers encourage their users toward high levels of self-revelation.

The danger to which an individual faces exposure to the possibly of breaches and thievery, as a user of social media services, is mostly known. Nevertheless,

this study confirmed the privacy paradox with respect to online self-revelation, which states that although users are aware of the hazards of self-revelation, they do not adjust their actions accordingly. Younger users publish more information on the Internet than older ones do. Gender differences showed women reveal more information than their male counterparts do (see Prommer et al., 2009).

The confirmed slight correlation between awareness of data security and educational level can be explained: Higher education may be accompanied by a higher level of information literacy, leading to a better assessment of privacy risks. To protect their privacy, most respondents stated they will reveal less information in the future. Furthermore, others want to ensure their information is only shared with specific circles. This method is popular, but it runs the risk the assumed audience differs from the actual one (especially for a large circle of friends).

Overall, the results suggest the necessity for increased political action to protect users' privacy. Our goals should be to teach everyone more advanced skills in how they can work securely with their online media, and also to determine ways we can form the necessary statutory framework allowing us to protect sensitive personal information from future exploitation – by advertisers or by any government.

References

Altman, I. (1977). Privacy Regulation: Culturally Universal or Culturally Specific? *Journal of Social Issues, 33*(3), S. 66–84.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9).

BITKOM. (2011). *Studie Soziale Netzwerke – zweite, erweiterte Studie*. Abgerufen am 29. 09 2014 von bitkom.org: http://www.bitkom.org/de/publikationen/38338_70897.aspx

Boyd, D. (2008). *Taken Out of Context. American Teen Sociality in Networked Publics*. University of California, Berkeley.

Boyd, D., & Hargittai, E. (2010). Facebook privacy setting: Who cares? *First Monday, 15*(8).

Boyd, D., & Marwick, A. (2011). Social Steganography: Privacy in Networked Publics. *Annual Conference of the International Communication Association*. Bosten, MA, USA.

Boyle, K., & Johnson, T. J. (2010). MySpace is your space? Examining self-presentation of MySpace users. *Computers in Human Behavior, 26*(6), S. 1392–1399.

Burgoon, J. K., Parrott, R., Le Poire, B. A., Kelley, D. L., Walther, J. B., & Perry, D. (1989). Maintaining and Restoring Privacy through Communication in Different Types of Relationships. *Journal of Social and Personal Relationships, 6*(2), S. 131–158.

Butler, E., McCann, E., & Thomas, J. (2011). Privacy Setting Awareness on Facebook and Its Effect on User-Posted Content. *Human Communication, 14*(1), S. 39–55.

Cho, H., & Larose, R. (1999). Privacy Issues in Internet Surveys. *Social Science Computer Review, 17*, S. 421–434.

Christofides, E., Muise, A., & Desmarais, S. (2009). Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? *CyberPsychology & Behavior, 12*(3), S. 341–345.

Cozby, P. C. (1973). Self-disclosure: A literature review. *Psychological Bulletin, 79*(2), S. 73–91.

DIVSI. (23. 05 2014). Jeder zehnte ist vorsichtiger geworden, die Mehrheit reagiert eher gleichgültig:Abhören? Egal, ich habe nichts zu verbergen!

Eiermann, M. (12. 06 2013). *Eine unheilige Allianz*. Abgerufen am 05. 08 2014 von theeuropean.de: http://www.theeuropean.de/martin-eiermann/7017-nsa-ueberwachung-und-soziale-netze#

Haferkamp, N., & Krämer, N. C. (2010). Online Self-presentation. Balancing Privacy Concerns and Impression Construction on Social Networking Sites. In K. Drotner, & K. C. Schrøder (Hrsg.), *Digital Content Creation: Perceptions, Practices & Perspectives* (S. 129–146). New York: Peter Lang.

Joinson, A. N. (2001). Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *European Journal of Social Psychology, 31*, S. 177–192.

Lewis, K., Kaufman, J., & Christakis, N. (2008). The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network. *Journal of Computer-Mediated Communication, 14*(1), S. 79–100.

Margulis, S. P. (2003). Privacy as a Social Issue and Behavioral Concept. *Journal of Social Issues, 59*(2), S. 243–261.

Morrison, S., & Gomez, R. (2014). Pushback: The Growth of Expressions of Resistance to Constant Online Connectivity. Washington, USA.

Nosko, A., Wood, E., & Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of FACEBOOK. *Computers in Human Behavior, 26*(3), S. 406–418.

O'Harrow Jr., R., Nakashima, E., & Gellman, B. (08. 06 2013). *U.S., company officials: Internet surveillance does not indiscriminately mine data*. Abgerufen am 02. 08 2014 von washingtonpost.com: http://www.washingtonpost.com/world/national-security/us-company-officials-internet-surveillance-does-not-indiscriminately-mine-data/2013/06/08/5b3bb234-d07d-11e2-9f1a-1a7cdee20287_print.html

Palen, L., & Dourish, P. (2003). Unpacking "Privacy" for a Networked World. In V. Belotti (Hrsg.), *SIGCHI Conference on Human Factors in Computing Systems* (S. 129–136). Ft. Lauderdale, Florida, USA: ACM New York.

Patchin, J. W., & Hinduja, S. (2010). Trends in Online Social Networking: Adolescent Use of MySpace over Time. *New Media & Society, 12*(2), S. 197–216.

Paukner, P. (18. 07 2012). *Facebook durchsucht Chat-Protokolle*. Abgerufen am 18. 09 2014 von sueddeutsche.de: http://www.sueddeutsche.de/digital/privatsphaere-im-netz-facebook-durchsucht-chat-protokolle-nach-straftaten-1.1411552

Petronio, S. (2002). *Boundaries of Privacy: Dialectics of Disclosure.* Albany: State University of New York Press.

Prommer, E., Brücks, A., Mehnert, J., Neumann, H., Räder, A., & Roßland, F. (2009). *„Real life extension" in Web-basierten sozialen Netzwerken Studie zur Selbstrepräsentation von Studierenden in studiVZ.* Potsdam.

Rössler, B. (2001). *Der Wert des Privaten.* Frankfurt am Main: Suhrkamp.

Schenk, M., Niemann, J., & Reinmann, G. (2012). *Digitale Privatsphäre – Heranwachsende und Datenschutz auf Sozialen Netzwerkplattformen.* (A. Roßnagel, Hrsg.) Düsseldorf: Vistas.

Spiegel Online. (03. 04 2013). *Soziales Netzwerk: Facebook verliert junge Nutzer in Deutschland und USA*. Abgerufen am 28. 09 2014 von spiegel.de: http://www.spiegel.de/netzwelt/web/nutzerzahlen-von-socialbakers-jugend-wendet-sich-von-facebook-ab-a-892266.html

Stiftung Warentest. (24. 03 2010). *Soziale Netzwerke: Datenschutz oft mangelhaft*. Abgerufen am 29. 09 2014 von test.de: http://www.test.de/Soziale-Netzwerke-Datenschutz-oft-mangelhaft-1854798-0/

Taddicken, M. (2008). *Methodeneffekte bei Web-Befragungen. Einschränkungen der Datengüte durch ein "reduziertes Kommunikationsmedium"*. Köln: Herbert von Halem Verlag.

Taddicken, M. (2010). Die Problematik der Selbstoffenbarung im Social Web. Theoretische Verortung und Forschungsstand. *Zeitschrift für Kommunikationsökologie und Medienethik, 1*, S. 143–153.

Taddicken, M. (2011). Selbstoffenbarung im Social Web Ergebnisse einer Internet-repräsentativen Analyse des Nutzerverhaltens in Deutschland. *Publizistik, 56*(3), S. 281–303.

Taddicken, M., & Jers, C. (2011). The Uses of Privacy Online: Trading a Loss of Privacy for Social Web Gratifications? In S. Trepte, & L. Reinecke (Hrsg.), *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (S. 143–156). Heidelberg: Springer-Verlag.

Taraszow, T., Aristodemou, E., Shitta, G., Laouris, Y., & Arsoy, A. (2010). Disclosure of personal and contact information by young people in social networking sites: An analysis using Facebook profiles as an example. *International Journal of Media & Cultural Politics, 6*(1), S. 81–101.

Thoma, J., & Greis, F. (25. 07 2013). *NSA bestätigt Existenz von zwei Prism-Programmen*. Abgerufen am 05. 08 2014 von golem.de: http://www.golem.de/news/abhoeraffaere-nsa-bestaetigt-existenz-von-zwei-prism-programmen-1307-100624.html

Utz, S., & Krämer, N. C. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 3*(2).

Wagner, U., Brüggen, N., & Gebel, C. (2010). Persönliche Informationen in aller Öffentlichkeit? *Jugendliche und ihre Perspektive auf Datenschutz und Persönlichkeitsrechte in Sozialen Netzwerkdiensten*. München.

Westin, A. F. (1967). *Privacy and Freedom.* New York: Atheneum.

Westin, A. F. (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues, 59*(2), S. 431–453.